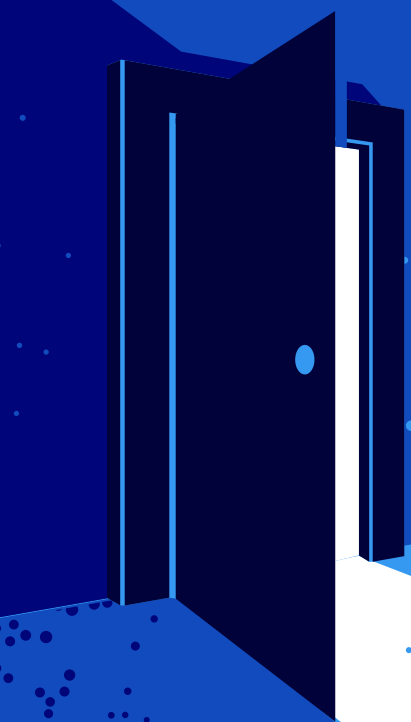
DATA PRIVACY DAY 2025

Privacy Culture Toolkit



TrustArc

Data Privacy Day 2025 calls for a renewed commitment to fostering a strong culture of privacy within organizations. The Privacy Culture Toolkit is your comprehensive resource to operationalize privacy best practices, empower employees with essential training, and establish clear accountability. Designed with privacy leaders in mind, this toolkit includes ready-to-use templates and guides to help you define roles, educate your workforce, and measure data subject requests effectively. Whether you're building foundational practices or enhancing an existing program, this toolkit provides the templates you need to integrate privacy into the heart of your organization's culture.

Table of Contents

Privacy Job Description Template

Depending on the size of the organization seeking to hire a privacy professional, or add further resources to their privacy office, it is recognized that staff may be appointed at varying degrees of seniority and experience. However, there are a number of constants that it is important to ensure are covered in any job description for a Chief Privacy Officer / Data Protection Officer role and this template aims to offer a comprehensive list of those which are key to include in any privacy related job description and those which are optional based on sector, region etc.

The privacy office in any organization should oversee all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the privacy of, and access to, personally identifiable information in compliance with all applicable privacy laws and the organization's information privacy practices.

The nature of privacy work involves close links between information technology and legal teams and wherever you choose to place your privacy team, they will need independence and a clear reporting line into the board.

There are no hard and fast rules surrounding the level of seniority of staff, or the structure of the privacy office, this will depend on a number of factors including the size of your organization, the nature of your business and budget. Listed below are detailed key accountabilities and person specification activities that can be utilised in the formulation and tailoring of a privacy job description to suit your needs. Where possible these have been split to three levels of Senior, Middle, and Junior management and are labeled accordingly.

Higher Management

Skill and Accountability

- Develop and implement processes to identify and address evolving privacy and data protection risks inherent in the Company's operations and in the development of new products and services.
- Design, implement and execute company-wide data privacy processes and procedures. Continually updating such processes and procedures as necessary.
- Ensure organizational compliance and conformance with privacy / data protection principles and highlight key risk areas to the board.
- Work with organization senior management and corporate compliance officer to establish an organization-wide Privacy Oversight Committee.
- Manage the organization's information and archiving process, providing advice and guidance to users on the retention schedule, storage requirements and managing the relationship with the off-site archiving and storage provider.
- Provides development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management and administration, the Privacy Oversight Committee and legal counsel. Provide information and guidance on the processing of all personal data.

CONTINUED →

- Maintain and establish a register of data owners for sets of information and educate the data owners on their responsibilities (what is data, how is it used, who has access to it).Maintain data flow maps as necessary.
- Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities.
- Maintains current knowledge of applicable privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Guides staff and project management in conducting documented Privacy Impact Assessments including both risk analysis and mitigation.
- Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
- Oversees, directs, delivers, or ensures delivery of initial and privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.
- Works with legal counsel and management, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

Person Specification

ESSENTIAL

- Strong leadership skills
- Ability to think strategically and to develop a multi-year, multi-faceted plan to address data protection and privacy risks.
- Proven, deep expertise in interpreting and applying global laws and regulations pertaining to data protection and privacy, with a nuanced understanding of jurisdictional differences in the approach to regulation. Specific experience developing and implementing measures to comply with EU data protection requirements in a large global organization strongly preferred.
- Legal degree, masters level education in business fields or other relevant advanced degree.
- Certification in privacy (CIPP, CHP, CHPS) and/or security (CISSP, CHS).
- 10+ years' experience leading privacy/ security initiatives.
- Ability to distill complex and often ambiguous legal concepts into effective operational solutions.
- Strong personal, analytical and communications skills.
- Strong drafting and negotiation skills.
- Demonstrated ability to translate privacy and security regulations and/or standards into workable and implementable solutions.
- Proven experience with change management in an international organization.

DESIRABLE

- Knowledge or expertise in IT protocols related to information security, data lifecycle management.

CONTINUED →

Mid Management

Skill and Accountability

- Manage privacy / data protection compliance and advise on legal requirements and best practice.
- Define, update and maintain the retention schedule and physical items inventory log.
- Work closely with Legal to review, interpret, comment and provide leadership on proposed and enacted regulations and industry-best practices.
- Develop and implement a Privacy Impact Assessment process.
- Work closely with the Legal, Product, ITC and other teams to identify and address data privacy issues or concerns in new or existing products and services, including conducting formal privacy impact assessments.
- Works with organization administration, legal counsel, and other related parties to represent the organization's information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standards.
- Interpret and provide guidance to the organisation on forthcoming and actual changes to relevant legislation on privacy and data protection.
- Reviews all system-related information security plans throughout the organization's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.
- Develop training strategy and materials and conduct company-wide training to ensure that employees are well-informed on key privacy issues.
- Undertake systematic privacy / data protection compliance audits, including any third party premises where appropriate.
- Responsible for ensuring appropriate responses are sent to all requests for access to information that are received by the organization.
- Be the lead contact with the relevant regulator with regard to potential complaints and breaches, ensuring that requests for information are properly handled.
- Assist with investigations into complaints about breaches of the act and undertake reporting/ remedial action as required.
- Maintain a log of any incidents and remedial recommendations and actions.

Person Specification

ESSENTIAL

- Bachelor's degree.
- CIPP certification.
- 5+ Years' experience working in a privacy or aligned field.
- Demonstrated organization, facilitation, communication, and presentation skills.
- Ability to simplify and teach others privacy-related concepts.

DESIRABLE

- Information security experience.

CONTINUED →

Junior Management

Skill and Accountability

- Develop, implement and enforce a suitable and relevant Privacy / Data Protection Policy and ensure it is reviewed on an annual basis.
- Advise on information good practice and standards related to the organization's overall ICT strategy needs, including business continuity requirements, and participate in any future information projects.
- Advise on and negotiate data privacy issues with third parties. Ensure compliance with all applicable contracts.
- Provide information and guidance on the processing of all personal data.
- Process, co-ordinate and respond to all requests for information.
- Maintain data flow maps as necessary.
- Maintain the organization's annual notification with the relevant regulator (EU).
- Establish and administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- Perform initial and periodic information privacy risk assessments and conduct related ongoing compliance monitoring activities in coordination with the entity's other compliance and operational assessment functions.
- Ensure that developments in data protection requirements and legislation are tracked and that the organisation is in apposition to comply with future requirements.
- Develop methods (processes) and guidance as needed with emphasis on business/function-specific activities, and fosters the development of new policies as necessary.
- Monitor laws, regulations, and contracts associated with the management and control of personal and sensitive data processed within the business/function.
- Extend privacy expertise to promote understanding and compliance across internal businesses functions and with external stakeholders.
- Manage emerging privacy events to resolution.

Person Specification

ESSENTIAL

- Bachelor's degree.
- 3+ years' experience working in a privacy related role.
- Good communication and negotiation skills.
- Ability to purvey complex concepts in a simple manner.
- Ability to multi-task and work effectively in a small team environment.

DESIRABLE

- CIPP Certification.

Maintaining Roles and Responsibilities for Individuals Responsible for Data Protection

Data Protection Officer: An Overview

The Data Protection Officer is an expert in the company's data privacy protection. They take care of privacy compliance and proper handling of personal data, including secure collection, processing, and deletion of personal information. While the European Union's General Data Protection Regulation (GDPR) often comes to mind in discussions about DPOs, it is important to note that several other jurisdictions, including Brazil, China, New Zealand, the Philippines, and the UAE, also mandate the appointment of a DPO under specific circumstances. The DPO is known by other titles under different privacy laws.

Such a person who is appointed as a data protection officer may be hired externally, through a service contract, or maybe designated internally within the company. Although most privacy laws do not specify the qualifications for appointing an individual as a DPO, there is, however, a consensus that a DPO should be someone who is well-equipped with the basic knowledge of privacy laws, information security, and business administration. Additionally, they must continue their education and training to continually meet the legal requirements. The DPO's role extends beyond mere legal expertise; they should also possess the ability to instill a robust data protection culture within the organization. Consequently, an ideal DPO should be well-versed in multiple disciplines.

The key requirement of a DPO's office is its independence. One of the methods to ensure independence is to appoint such an individual as a DPO, who does not have a conflict of interest. Thus, the appointment of a Director, CEO, CIO, CSO, or departmental heads of marketing or sales is usually discouraged, as individuals holding these positions are the ones who have a direct interest in processing personal information. Secondly, to ensure the independence of the DPO's office, they should directly report to the highest level of management. Thirdly, organizations should refrain from providing instructions to the DPO on how to perform their job. Lastly, DPOs should not face penalties or dismissal for fulfilling their duties.

Roles and Responsibilities: Suggested Practices

1. To inform the controller or processor processing personal data of their obligations under the privacy law applicable to them and other relevant data protection provisions.

2. To monitor compliance with the relevant data protection provisions. This will include:
   - → The assignment of responsibilities;
   - → Training and awareness-raising of employees;
   - → Related audits.

3. To provide advice on Data Protection Impact Assessments (DPIAs) and monitor their performance.

4. To cooperate with the Supervisory Authority. Acting as the point of contact for, and consulting with, the Supervisory Authority on issues related to the processing of personal data; including prior consultation with the authority as necessary.

5. To be accessible by the data subjects of the controller or processor on all issues related to the processing of their data and their rights under the applicable law.

6. To define the means of processing when working jointly with other controllers or with processors. In other words, the practices required to ensure legal processing are both defined and communicated when bodies other than the controller are involved in the processing of personal data.

CONTINUED →

7. Have due regard to the risk associated with the processing operations when exercising tasks. They should take into account the nature, scope, context, and purposes of the processing.

8. To serve as the contact point for data subjects on privacy matters, including DSARs, handling of inquiries, complaints, and correction of personal information.

9. To advise on privacy matters and act as the first point of contact for advice on privacy matters.

10. To manage, survey, and improve data processing as well as establish a data protection plan

11. To establish and implement a privacy policy along with maintaining material related to data protection.

12. To ensure the destruction of personal data once the purpose of the processing is complete or the retention period expires.

Compliance Considerations

The concept of a data protection officer has been popularized by the GDPR, now a number of jurisdictions also require or encourage organizations to appoint a DPO under specific circumstances. Regardless of whether required by regulations, organizations managing sensitive personal data are strongly encouraged to designate a DPO or a similar role to oversee data protection and privacy. There is flexibility in how this function can be structured, either by appointing a dedicated individual or by assigning the role to someone within the team who can manage it alongside their other responsibilities, provided they have the autonomy to perform their duties independently. Below are examples of jurisdictions that require organizations to appoint a DPO in some capacity:

1. **Australia** requires privacy officers to:
   - → Maintain records of personal information held by the agency.
   - → Liaise with the OAIC.
   - → Annually audit the organization's performance against its privacy management plan.

2. In the **Philippines**, individuals must be appointed who are accountable for the organization's compliance with the law and are required to:
   - → Monitor personal information controller's (PIC) and personal information processor's (PIP) compliance with the DPA, 2012.
   - → Analyze and check compliance of processing activities, including issuance of security clearances to and compliance by third-party service providers.
   - → Ascertain renewal of accreditations and certifications necessary to maintain the required standards in personal data processing.
   - → Advocate for the development, review, and revision of policies, guidelines, projects, and programs of the PIC or PIP relating to privacy and data protection.

3. **Ukraine's** Data Protection Law requires the responsible person to:
   - → Organize the work related to personal data protection.
   - → Inform and advise the controller or processor on observance of the legislation.
   - → Cooperate with the Ukrainian Parliament Commissioner for the protection of human rights and appointed officials on compliance.

4. **India's** DPDPA under section 11 requires a significant controller to appoint a Data Protection Officer based in India, who will:
   - → Represent the Significant Controller under the provisions of this Act;
   - → Be an individual responsible to the Board of Directors or similar governing body of the Significant Controller;
   - → Act as the point of contact for the grievance redressal mechanism under the provisions of this Act.

If the organization decides not to appoint a DPO, it should document the reasons for this decision to demonstrate to regulators that the choice was carefully considered.

Employee Training Requirements

Overview

In the United States, there are three categories of laws that regulate the privacy and security of personal information. The first category includes consumer data privacy laws such as CCPA, Virginia's CPDA, and others. The second category involves sector-specific data protection laws such as HIPAA for the protection of health data, GLBA for the protection of financial information, and other laws that regulate privacy in education, driver's licenses, and so on. The third category includes data security and breach notification laws such as the New York Shield Act. One of the common features of all these laws is that they require covered businesses to implement technical and organizational measures for data security and privacy. One of the most common organizational measures to ensure data privacy is to train employees about the dos and don'ts of data privacy laws.

Employee training requirements under the U.S. state consumer privacy laws

1. Section 1798.130(a)(6) of California's CCPA requires that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPAare informed of the relevant requirements, including how to direct consumers to exercise their rights. Furthermore, Section 1798.135(c)(3) provides that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance are informed of the requirements under sections 1798.120 and 1798.121 around the right to opt-out of sale or sharing of personal information, the right to limit the use and disclosure of sensitive personal information, and how to direct consumers to exercise that specific right. Additionally, Section 999.317 of the Regulations reiterates the requirement to inform all individuals handling consumer inquiries of CCPArequirements and how to direct consumers to exercise their rights.
2. Other privacy legislation from the US States has taken a slightly different approach by requiring businesses/controllers to ensure certain levels of data security measures to protect personal information. These measures are not detailed in any legislation, hence, it is up to the business or controller to decide on what specific measure needs to be implemented. However, employee training has always been regarded as crucial for data privacy and security practices. By educating one's staff, a business or controller can significantly enhance their data security posture to better comply with state privacy laws.

Suggested Practices

1. Understand the requirements of the privacy laws applicable to the business. For instance, all employees managing compliance with CCPA or handling consumer rights requests must have a thorough knowledge of all the applicable requirements of law and should know how to direct consumers to exercise their rights.
2. Ensure that all employees within your organization who are implementing, managing, or overseeing compliance receive training. These employees could include executives, managers, human resources, marketing, sales, and IT employees.
3. Ensure that the training material is easily comprehensible and free from legal jargon. Ideally, employees should walk away with an easy-to-use understanding of their role in the company's compliance with the applicable privacy laws.

CONTINUED →

4. The training should include all the practical requirements of the law, including but not limited to privacy notices, privacy rights, and data governance.

5. For trainers, there is no minimum qualification. However, a person with previous, relevant experience in training employees should be assigned this task. You may also consider consulting with a third party for training.

6. The training material may include the following items but should not be limited to:

   - Introduction to the US privacy landscape
   - Introduction to laws applicable to your business
   - Basic understanding of data privacy in the US
   - How to process personal data lawfully
   - Individual rights and requests
   - Data security practices
   - Data breach notifications
   - Data protection for US businesses working globally

Employee Privacy Training Policy Template

1. Purpose

Explain why employee training policy is needed for your organization and what benefits it should bring.

The purpose of the [Company name] Privacy Training Policy is to set the standards for employee training. The below-stated policy has been documented and implemented to comply with legal and contractual requirements and to ensure that all employees involved in handling the personal information of our [consumers, customers, and clients] are aware of what is expected of them and take responsibility for protecting the privacy of personal information.

2. Scope

List the employees, or categories of employees who shall receive the training under this policy.

This policy shall apply to [executive management, employees of the HR department, Marketing, etc].

The scope of this policy shall ideally depend on two things, first the privacy law that applies to your business and second, the data privacy practices within your organization. Employees who are involved in data processing activities, employees who shall be receiving and responding to DSARs, and employees who are involved in implementing, overseeing, or managing compliance should be included within the scope of this policy. However, basic training involving data privacy practices should be made mandatory for all employees.

3. Responsibility for training

List the department or categories of employees who shall be responsible for ensuring that training is imparted to all the individuals to whom this policy applies and what responsibilities they shall have in this regard.

[Company's name] [Privacy Office / HR department / Legal Department] shall be responsible for conducting the training given under this policy. They shall also be responsible for:

- Creating the content for such training that suits the business requirement and is in line with employees' roles and responsibilities within the organization.
- Developing methods and procedures to ensure that employees have understood the training material. These methods may include multiple-choice questions, mock tests, and interviews.
- Identifying any special role-based training
- Creating metrics and reports on training activities.
- Developing a timeline in which the training needs to be completed.
- Establishing procedures where assigned training is not completed by any employees

Managers of each department shall be responsible for ensuring that employees under their supervision are assigned the correct training.

4. Training Procedure

New Hire Training – [Company name] will set baseline requirements for all personnel to complete training upon hire, including data privacy, security, [insert other training as applicable, this could be specific, such as "CPRA compliance"]. All personnel shall complete the required onboarding training within [thirty days] of hire and before receiving access to consumer data. Exceptions may be granted upon request and a showing of need but will only be extended for extenuating circumstances for a limited time or scope.

Refresher Training – [Company name] will provide ongoing training on a regular cadence, no less than annually. This training is to reinforce previously learned material and will incorporate new material as necessary, as determined by the responsible department or person. All personnel are responsible for completing this training unless their hire date is within ninety (90) days of the start date of the refresher training.

Refresher training could include Attorney General regulations, outcomes from civil claims, lessons learned from requests processed by the Company.

CONTINUED →

Ad hoc Training – [Company name] will provide ad hoc training as the circumstances require. This training is to address changes in the industry, operations, environment, law/regulations, or situational as determined by the responsible department or person. This training may be directed to a person, department, or the company as a whole.

Ad hoc training may be required if the Company launched a new way by which consumers may submit requests if there have been changes to business practices that impact the responses that would be given in response to DSARs.

Mitigation Training – At times, the responsible department or person may identify a need to provide training to address an error that occurred or behavior that needs correction. This may be reflected in an employee's personnel file, may be linked to disciplinary action, and/or may be provided on a one-on-one basis or to a group.

This type of training would likely apply to those employees who are customer-facing and/or may be receiving or handling a CPRA request. Examples include if the employee did not recognize that a request was being made and did not forward it to appropriate teams for handling, or where a response was inaccurate, incomplete, or not handled within legislative deadlines.

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Revision History

See chart below:

Version History	Published	Author	Description of Change

Core Training Program Considerations

Training Objectives:

All employees should:

- Have a general awareness of the organization's privacy rules;
- Know that sensitivity is needed when handling personal data;
- Know how to obtain a copy of the organization's privacy policy;
- Be able to direct a customer to the privacy policy; (regional awareness when necessary)
- Know where to direct or escalate a privacy related question or concern; (regional awareness when necessary)
- Know what to do if they become aware of a breach;
- How to manage data within the retention schedule;
- Know how to contact the Privacy Office.

Employees that handle personal data should:

- Be required to understand what is and what is not personal data;
- Have a good understanding of corporate policies;
- Understand the concepts of consent and purpose, including how they impact the processing of personal data (required for privacy-sensitive roles);
- Be able to recognize privacy situations and know how to respond;
- Understand the implications of a breach to the organization;
- Be aware of the organization's breach response protocols (optional).

Employees that handle sensitive personal data or whose role requires greater privacy knowledge should be required to:

- Understand and be required to apply privacy policies to job functions;
- Be able to advise and deal with questions in their functional area about processing of personal data;
- Be able to address a breach response (optional);
- Be able to address escalated access requests or other second level complaints (required for privacy-sensitive roles);
- Be able to respond in more detail about policy and relevant procedures (required for privacy-sensitive roles);
- Have a working level knowledge of privacy legislation (optional);
- Know when and how to escalate issues to the Privacy Officer.

Program Delivery:

In choosing a training delivery method, consider:

- The learning objectives;
- Number of learners;
- The organization's ability to efficiently deliver the material;
- Types of learners present: visual learners; audio learners; hands-on learners.
- Ability to record knowledge and completion.

CONTINUED →

Delivery mechanisms:

- Lecture-based event;
- Classroom training;
- Small in-person workshops;
- Role-playing real world scenarios;
- Online or computer-based modules;
- Multimedia presentations that use graphics, videos, photos, and animation;
- Paper-based self-study training packages;
- Video, DVD, or CD-based training;
- Informal department meetings with the Privacy Office;
- Privacy Intranet website.

Make the program user-friendly:

- Make training relevant, personal, and timely;
- Gear lessons to the comprehension levels of participants;
- Address just a few key issues at a time;
- Break up the training into manageable modules;
- Avoid including technical or regulatory content that doesn't meet the "need-to-know" test.

If using e-learning, consider mechanisms to engage the viewer:

- Drag and drop features where the viewer has to select the correct answer and drag it to another part of the screen;
- Video elements to give the viewer a break from reading;
- Gamification using video game design and elements.

If using external instructors:

- Conduct a pre-briefing to cover expected standards of service and delivery, e.g. on: course expectations; anticipated participant reactions; and the dynamics of the current workforce culture.
- Have the course content and exercises reviewed by an experienced training expert;
- Consider external conferences, in person and webinar to improve knowledge, earn credits and networking experiences;
- Consider using business unit leaders to conduct training rather than the privacy office.

Training Topics:

- **A general overview of privacy:** What is it? What does privacy mean to the employee, contractor or vendor? What does privacy mean to the customer, client, etc.?
- **The organization's commitment to privacy:** Include corporate mission statements.
- **A brief legal overview** (optional): The names of the relevant laws; (regional breakdown when necessary), principles and objectives of relevant privacy legislation.
- **Consumer concerns or issues** (optional): Types of complaints the organization has received to date.
- **Privacy risks:** Data breaches (optional); Inappropriate uses of personal data (required); The consequences of complaints against the organization (optional).
- **Personal data:** What it is; What it is not; What is sensitive personal data (optional).
- **Corporate policies:**
  - → Review key corporate policies;
  - → Review role of the corporate privacy office, if applicable;
  - → Provide contact information for the Privacy Officer and/or key information security and privacy contacts;
  - → Explain when and how to escalate concerns or complaints;
  - → Reinforce corporate personal data handling procedures such as (optional): collection; use; internal and external sharing and disclosures; retention; security and destruction; breach response; use of technology, including mobile devices and social media.

CONTINUED →

- **Employee privacy policies** (optional): Explain the importance of the policy; Provide guidance as to where to seek additional information regarding the employee privacy policy.
- Employee, contractor, vendor roles, and responsibilities.

Review Training Annually:

Training materials and programs are updated annually to:

- Reflect changes in legislative, regulatory, and industry requirements (optional);
- Integrate learnings from findings and orders (optional);
- Adopt 'best practices' as identified by trade associations, etc. (optional);
- Reflect new requirements based on new or updated: policies and procedures; software or hardware (optional); or changes in internal and external risks security technology (optional);
- Address specific learnings from an event such as a customer complaint or a data breach (optional).

Training & Awareness Checklist for Working with AI

- Communicate to and train employees on their responsibilities when working with AI systems:
  - → Inform employees about the implications and consequences of using AI tools in the workplace (e.g., outputs of certain tools can be inaccurate).
    Keep in mind that the use of AI and concept of ethics may be a novel concept to some employees.
  - → Clearly communicate to employees if there are tools specifically recommended or prohibited.
    Provide clear guidance on how employees can or cannot use AI tools to perform their essential job functions.
  - → Remind employees that relevant legal obligations continue to apply to the use of new tools.
  - → Warn employees against inputting personal data, confidential business information, trade secrets or other sensitive data into AI systems.
  - → Consider specific training to help employees understand and mitigate legal liability in the use of certain AI tools, particularly for businesses in a regulated industry.
  - → Update employee resources, including employee handbooks to reflect policies regarding AI use.
- Establish and enforce development guidelines to hold employees dealing with AI systems accountable.
- Establish and communicate protocols for employees using AI applications on work-issued devices:
  - → Advise employees which settings or permissions are acceptable.
- Provide employees with resources that address the responsible use of all types of automated processing.
- Hold training sessions and workshops on different aspects of AI, such as:
  - → Ethics and bias
  - → Data minimization
  - → Data accuracy or inaccuracy
  - → Transparency & explainability
  - → Data security
- Provide specialized training for employees responsible for human intervention processes:
  - → Develop, document and train all human intervention processes before the launch or use of an AI system so that customers can exercise such an alternative from day one.
- Set up refresher training at regular intervals to keep employees up-to-date on current legal restrictions or permissions and emerging risks associated with AI systems.

Data Subject Request Metrics

Overview

§7102 of CPRA regulation requires companies that process large columns of data about Californians to post metrics regarding data subject requests publicly. California's privacy law was the first law that required companies to disclose information about their DSR process publicly. The California Attorney General enacted a regulation that requires companies that bought, received, sold, or shared personal information of ten million or more California residents in a calendar year to disclose DSR metrics in their privacy notices publicly. Thus businesses are required to disclose the number of access requests, opt out requests, deletion requests, and "Do Not Sell" requests that the business has received. The records must be maintained for at least twenty-four months, during which time, reasonable security measures must be in place to protect the records. The business is not required to retain personal information solely to fulfill a consumer request, however, where a consumer makes a request, the business must maintain a record of it.

Other US state privacy laws do not have this requirement.

Maintenance of records

1. Records of consumer requests may be maintained in a ticket or log format, provided that the ticket or log includes the following information:

   - Date of request;
   - Nature of request;
   - How the consumer made the request;
   - The date on which the business responded to the request;
   - Nature of the response provided by the business;
   - The basis for the denial of the request if the request was denied in whole or in part.

2. Metrics relating to consumer requests:

   A business that buys or sells, or receives or shares for a commercial purpose, the personal information of 10 million or more consumers in a calendar year must compile metrics relating to consumer requests handled in the previous calendar year. Such metrics must include:

   - Number of requests to delete personal information that the business received, complied with in whole or in part, and denied;
   - Number of requests to correct personal information that the business received, complied with in whole or in part, and denied;
   - Number of requests to know received, complied with in whole or in part, and denied;
   - Number of requests to opt-out of the sale or sharing of personal information that the business received, complied with in whole or in part, and denied;
   - Number of requests to limit the use of sensitive personal information that the business received, complied with in whole or in part, and denied;
   - The median or mean number of days within which the business substantively responded to requests to delete, correct, know, opt-out, and limit.

3. Public disclosure of metrics:

   A business that buys or sells personal information, or receives or shares personal information for a commercial purpose, of 10 million or more consumers in a calendar year must disclose, by July 1 of each calendar year, metrics it has compiled relating to consumer requests. The metrics must be disclosed within the business' privacy policy, or posted on the business' website and accessible from a link included in its privacy policy. A business may choose to disclose the number of requests that it denied in whole or in part where the request:

   - Was not verifiable;
   - Was not made by the consumer;
   - Called for information exempt from disclosure requirements;
   - It was denied on other grounds.

4. Training policy:

   Businesses must establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests are informed of the requirements for such handling.

5. Other considerations:

   For simplicity purposes, a business may choose to record and disclose metrics for requests received from all individuals, rather than requests received specifically from consumers. In this case, the business must state that it has done so in its disclosure and be prepared to provide consumer-specific metrics to the Attorney General upon request.

   Personal information maintained for recordkeeping purposes may not be used for any other purpose, except as reasonably necessary for the business to review and modify its processes for compliance with CPRA. Similarly, personal information maintained for recordkeeping purposes may not be shared with any third party, except as necessary to comply with a legal obligation.

   The retention of personal information for the sole purpose of recordkeeping, where the information is not used for another purpose, does not in itself constitute a violation of CPRA.

CONTINUED →

Sample disclosure

Consumer Request Metrics for the [insert previous calendar year] year:

1. Requests to delete:

   [insert number here] requests received;

   [insert number here] requests complied with, whether in whole or in part;

   [insert number here] requests denied; and

   The median or mean number of days within which we substantively responded to requests was [insert number of days here].

2. Request to correct:

   [insert number here] requests received;

   [insert number here] requests complied with, whether in whole or in part;

   [insert number here] requests denied; and

   The median or mean number of days within which we substantively responded to requests was [insert number of days here].

3. Requests to know:

   [insert number here] requests received;

   [insert number here] requests complied with, whether in whole or in part;

   [insert number here] requests denied; and

   The median or mean number of days within which we substantively responded to requests was [insert number of days here].

4. Requests to opt out of the sale/sharing of personal information:

   [insert number here] requests received;

   [insert number here] requests complied with, whether in whole or in part;

   [insert number here] requests denied; and

   The median or mean number of days within which we substantively responded to requests was [insert number of days here].

5. Requests to limit the use of sensitive personal information:

   [insert number here] requests received;

   [insert number here] requests complied with, whether in whole or in part;

   [insert number here] requests denied; and

   The median or mean number of days within which we substantively responded to requests was [insert number of days here].

Metrics to track

The below questionnaire can be used to track certain metrics for DSARs.

1. **Stage 1** *(Track visits to your privacy page)*
   - → How many visits to your privacy pages resulted in requests?
   - → What next steps do consumers take such as form submissions, emails, or phone calls)?
2. **Stage 2** *(Track DSAR submissions)*
   - → How many DSARs have you received both in aggregate and by user?
   - → How many requests were started and abandoned?
   - → How many types of DSAR requests have you received (Access requests, Deletion requests, Opt-out requests)?
3. **Stage 3** *(Request Verifications)*
   - → How often are you able to match DSAR requests with unique individuals?
   - → How often are you unable to verify or authenticate a request and thus unable to fulfill it?
   - → What's the proportion of requests from CA residents vs. non-CA residents?
   - → What's the proportion of requests from customers vs. non-customers?
   - → What proportion of the requests are abandoned at the verification stage?
4. **Stage 4** *(Request Completion)*
   - → How long does it take to complete a request? (mean or median)
   - → What proportion of requests are delivered within the 45-day window?
   - → How many people are involved in fulfilling a DSAR?
   - → How many systems are involved in fulfilling a DSAR?
   - → How does timing differ by type of DSAR, business unit, or team member?
   - → How many times have you needed to ask for an extension?
5. **Stage 5** *(Post-fulfillment)*
   - → Is there an uptick in purchase activity from customers who have received completed DSARs?
   - → Are you seeing higher engagement from consumers once you have delivered DSARs?

Do your regulatory research — better yet, let us do it.

Spending hours online searching and understanding privacy regulatory changes is time-consuming. Nymity Research does it for you, keeping you on top of the latest laws, regulations, standards, and operational best practices around privacy, across a multitude of jurisdictions.

Start your free trial

TrustArc